Abstract

The correctness of an exponentiation operation or other type of operation associated with a multi-party cryptographic protocol is verified using first and second proofs based on a randomized instance of the operation. A prover generates signals corresponding to information representative of the first and second proofs based on the randomized instance. The first proof is a so-called "blinded" proof that the operation has been correctly performed, configured so as to prevent leaks of information relating to the cryptographic protocol. The second proof is a proof that the first proof has been correctly performed by the prover. The proof information signals are transmitted from the prover to a verifier, and the verifier uses the signals to determine if the operation associated with the cryptographic protocol is valid. For example, the verifier in an illustrative embodiment generates an indication that the operation was correctly performed if the first and second proofs are acceptable to the verifier, generates an indication that the operation was not correctly performed if the first proof is not acceptable but the second proof is acceptable, and generates an indication of a cheating prover if the second proof is not acceptable. The verification protocol can be used in applications in which the prover is distributed across a number of different machines.